ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●郵送されたUSBメモリーからランサムウェアに感染…米国で攻撃発生、FBIが警告

https://japan.zdnet.com/article/35181884/
https://news.mynavi.jp/techplus/article/20220113-2248504/

このニュースをザックリ言うと・・・

- 1月7日(現地時間)、米IT系メディア「Bleeping Computer」等より、USBメモリーを郵送してランサムウェアに感染させようとする攻撃についてFBIから警告が出ていることが報じられています。

- 記事によれば、USBメモリーは米保健福祉省からの新型コロナウイルスに関する情報が入っていると偽るなどして送られているとの情報があり、接続したPCにマルウェアをダウンロードしてインストールさせる挙動をとり、最終的にはLAN上のPCをも標的としたランサムウェア攻撃を行うことが目的とされています。

- 既に2021年8月には運輸・保険業界の組織、同年11月には防衛業界の組織に当該USBメモリーが郵送されているとのことですが、2020年に同様の攻撃を行ったロシアのサイバー犯罪グループ「FIN7」が関与している可能性が指摘されています。

AUS便りからの所感等

- ファームウェア等へ細工を行ったUSBメモリーにより、マルウェア感染等を引き起こす攻撃の手口は「BadUSB」と呼ばれ、2014年にセキュリティ研究者によって発表されたもので、接続したPCに対してキーボードデバイスになりすまし、マルウェアのダウンロード等の不正なコマンドを入力・実行する仕組みになっています。

- この他にも、接続したPCに高圧電流を流して物理的に破壊する「USB Killer」と呼ばれるUSBメモリー型デバイスも発表されています。

- 2015年には、約300個のUSBメモリーを放置したところ、約半数が拾われてPCに接続されたとする実験結果が発表されています。

- 現行のUSBの仕様上、現状アンチウイルスでもこのような悪意のあるUSBデバイスを確実に検疫し、攻撃を完全に防ぐようなことは困難とされている模様であり、現状では組織内で使用するあらゆるUSB機器を厳密に管理下に置くとともに、身元が不明な相手から送られたデバイスを安易にPCに接続しないことが肝要です。

ZDNet Japan

USBメモリーを標的に送りつけて攻撃--挿入されたPCにランサムウェアをインストール

Liam Tung（Special to ZDNet.com）翻訳校正：編集部　2022-01-11 14:39

米連邦捜査局（FBI）は、サイバー犯罪集団がUSBメモリーを企業に郵送し、受け取った企業がそれをPCに接続すると、ネットワークにランサムウェアがインストールされる攻撃が米国で進行中であることを明らかにした。

このUSBメモリーを使った攻撃の手口は、「BadUSB」と呼ばれるものだ。問題のUSBメモリーは、米国の郵便公社と大手貨物運送会社であるUnited Parcel Serviceを使って送付されている。中身にはいくつかの種類があり、そのうちの1種類では、USBメモリーに新型コロナウイルスに関する情報が入っていると記された、米保健福祉省からのものを装った送付状が同封されている。また、Amazonからのものに見せかけて、ギフトカードとUSBメモリーが入った小包が送りつけられてくるケースもある。

BadUSB攻撃は、USB規格の汎用性を悪用した攻撃手法だ。この攻撃では、USBデバイスのファームウェアを書き換えることによって、デバイスをキーボードだと認識させて自動的にキー入力を行い、コンピューターにコマンドを実行させたり、OSが起動する前にマルウェアをインストールしたり、ネットワークカードに偽装してトラフィックをリダイレクトしたりすることができる。

●ドコモ・ソフトバンクが迷惑SMSの受信拒否機能発表、今春から開始

https://www.itmedia.co.jp/news/articles/2201/13/news152.html
https://www.nttdocomo.co.jp/info/news_release/2022/01/13_00.html
https://www.softbank.jp/corp/news/press/sbkk/2022/20220113_02/

このニュースをザックリ言うと･･･

- 1月13日(日本時間)、NTTドコモ(以下・ドコモ)とソフトバンクより、SMSによるフィッシング詐欺(スミッシング)を防止するための機能を提供することが発表されました。
- ドコモはahamoを含めた同社ユーザーに対し「危険SMS拒否設定」を3月中旬から提供予定としています。
- ソフトバンクもワイモバイル・LINEMOを含めたユーザーへ「なりすましSMSの拒否(差出人詐称SMSが対象)」「URLリンク付きSMSの拒否(携帯電話番号からのSMSが対象)」「迷惑SMSフィルター」を春頃に提供予定としています。

AUS便りからの所感

- いずれも一部機能については提供開始後に自動で有効となり、利用開始の手続き等は不要とのことです。
- 両社と同じく携帯電話キャリアのKDDI(au)と楽天モバイルからは1月18日時点で発表はないものの、近日中に同様のサービスを提供することが予想されます。
- キャリア各社とも既に迷惑メール対策のサービスは提供している一方、SMSについては、例えばドコモが「一括拒否」か「個別番号受信」が設定可能といった程度で、スミッシングに対しては効果的な対策が提供できていなかったとみられます。
- 今回の対策機能提供以後も、不審なSMSを受信する可能性は皆無ではないことに注意し、受信の際はリンクのURLのドメイン名以外にも、ネット上に報告がないか検索することによって判断し、慎重な行動をとるよう心掛けましょう。

ITmedia NEWS

迷惑SMSは受信拒否　ドコモとソフトバンクが春に機能追加へ　フィッシング詐欺対策で

2022年01月13日 16時30分 公開　[ITmedia]

NTTドコモとソフトバンクは1月13日、迷惑SMSの受信を拒否する機能の提供を今春に始めると発表した。SMSを使ったフィッシング詐欺「スミッシング」による被害を防止する。

不正なアプリのダウンロードやフィッシングサイトに誘導するURLなどを含むSMS、キャリアなどをかたる“なりすましSMS”などを判別してシャットアウトする機能。提供開始後に自動で稼働するため申し込みや利用開始の手続きは不要。使用料は無料。ahamoやLINEMOなどのサブブランドのユーザーにもサービスを提供する。

●「テプラ」のWi-Fi機能に脆弱性…本体ソフトウェアのアップデートを

https://news.mynavi.jp/techplus/article/20220114-2249040/
https://www.kingjim.co.jp/download/security/#sr01

このニュースをザックリ言うと･･･

- 1月13日(日本時間)、キングジム社より、同社「テプラ」の一部機種のWi-Fi通信機能に脆弱性が存在することが発表されました(同日、JPCERT/CCからも注意喚起が出されています)。
- 脆弱性が存在するのはテプラ PRO SR5900P / SR-R7900Pで、脆弱性の悪用により、Wi-Fiアクセスポイントにアクセスするための認証情報が無線LAN経由で奪取される可能性があるとされています。
- 同社では本体ソフトウェア等について脆弱性を修正したバージョンをリリースしており、アップデートを呼び掛けています。

AUS便りからの所感

- 同社からはパスワードマネージャー「ミルパス」についても保存されたパスワードが奪取される脆弱性が存在しているとし、こちらはサポートが終了していることから、使用を停止するよう推奨しています。
- 有線・無線に拘わらず、ネットワーク通信機能を持つ機器によっては、通常オフラインで使用する場合であっても、知らない間に通信機能が有効になり、外部からアクセス可能な状態となる可能性も考えられるため、そうした機器全てについて組織内での存在を把握したうえで、随時ベンダー情報を確認し、ファームウェア等のアップデートが行われ次第必ず適用を行うような管理体制を整えるべきでしょう。

TECHI Powered by マイナビニュース

ラベルプリンタ「テプラ」に脆弱性、アップデートを

2022/01/14 13:15　著者：後藤大地

脆弱性　キングジム　JPCERT/CC

JPCERTコーディネーションセンター（JPCERT/CC: Japan Computer Emergency Response Team Coordination Center）は2022年1月13日、「JVN#81479705: ラベルプリンター「テプラ」PRO SR5900P / SR-R7900P における認証情報の不十分な保護の脆弱性」において、キングジムのラベルプリンタ「テプラ PRO SR5900P」および「同SR-R7900P」に脆弱性が存在すると伝えた。この脆弱性を悪用されると、認証情報が漏洩する可能性があるとされている。